# ORDER FOR SUPPLIES AND SERVICES

| REQUISITION/REFERENCE NUMBER | PAGE | OF | PAGES |
|---|---|---|---|
| 000001P0 | 1 | | 3 |

| 1. DATE OF ORDER | 2. ORDER NUMBER | 3. CONTRACT NUMBER | 4. PDN NUMBER |
|---|---|---|---|
| 09/28/2022 03:55:12 PM EDT | 47QFRA22F0010 | 47QTCK18D0029 | |

FOR GOVERNMENT USE ONLY

5. ACCOUNTING AND APPROPRIATION DATA

| FUND | FUNCTION CODE | B/A CODE | CC-A | C/E CODE | FY | REGION |
|---|---|---|---|---|---|---|
| 285F | AF151 | AA20 | | H08 | | |
| **CC-B** | **PROJ./PROS NO.** | **O/C CODE** | **ORG. CODE** | **W/ITEM** | **PRT./CRFT** | |
| | | 25 | Q08FA000 | | | |

6. TO: CONTRACTOR (Name, address and zip code)

DELOITTE CONSULTING LLP 1919 N LYNN ST ARLINGTON, Virginia 22209-1742 United States
703-885-6000

7. TYPE OF ORDER

A. ☐ PURCHASE

Please furnish the following on the terms and conditions specified on the order and the attached sheets, if any, including delivery as indicated.

B. ☐ DELIVERY (For Supplies)

This delivery order is issued subject to the terms and conditions of the above numbered contract.

C. ☒ TASK ORDER (For Services)

This task order is issued subject to the terms and conditions of the above numbered contract.

| 8A. Data Universal Numbering System (DUNS) Number | 8B. Taxpayer Identification Number (TIN) |
|---|---|
| (b) (4) | (b) (4) |

9A. BUSINESS CLASSIFICATION

For-Profit Organization

| D. MODIFICATION NUMBER | AUTHORITY FOR ISSUING |
|---|---|
| P00000 | |

Except as provided herein, all terms and conditions of the original order, as heretofore mentioned, remain unchanged.

9B. START DATE: 09/28/2022

9C. COMPLETION DATE: 09/27/2023

10. ISSUING OFFICE (Address, Zip Code, and Telephone Number)

Denver Federal Center W 6th Avenue & Kipling Street Denver, Colorado 80225 United States Lauren N Pfarr (b) (6) lauren.pfarr@gsa.gov

11. REMITTANCE ADDRESS (MANDATORY)

DELOITTE CONSULTING LLP 1919 N. Lynn Street Arlington, Virginia 22209-1747 United States

12. SHIP TO (Consignee Address, Zip Code and Telephone Number)

National Protection & Programs Directorate Joseph Sheridan 1401 South Clark Street Arlington, Virginia 22202-0000 United States 202-857-2588

13. PLACE OF INSPECTION AND ACCEPTANCE

Joseph Sheridan 1616 North Fort Myer Drive Arlington, Virginia 22202-0000 United States 202-857-2588

14. REQUISITION OFFICE (Name, Symbol and Telephone Number)

GSA FAS AAS Region 08 Denver Federal Center W 6th Avenue & Kipling Street Denver, Colorado 80225 United States Diana E Zoppi (b) (6) diana.zoppi@gsa.gov

| 15. F.O.B. POINT | 16. GOVERNMENT B/L NUMBER | 17. DELIVERY F.O.B. POINT | 18. PAYMENT/DISCOUNT TERMS |
|---|---|---|---|
| Destination | | 09/27/2023 | Net 30 Days / 0% 0 Days |

19. SCHEDULE

| ITEM NUMBER (A) | SUPPLIES OR SERVICES (B) | QUANTITY ORDERED (C) | UNIT (D) | UNIT PRICE (E) | AMOUNT (F) |
|---|---|---|---|---|---|
| | See Continuation Page | | | | |

20. RECEIVING OFFICE (Name, Symbol and Telephone Number)

National Protection & Programs Directorate (202) 603-3769

TOTAL FROM 300-A(s)

GRAND TOTAL $2,505,324.30

21. MAIL INVOICE TO: (Electronic Invoice Preferred)

General Services Administration (FUND)
The contractor shall submit invoices electronically by logging into the ASSIST portal (https://portal.fas.gsa.gov),navigating to the appropriate award, and creating the invoice for that award. For additional assistance contact the ASSIST Helpdesk at 877-472-4877. Do NOT submit any invoices directly to the GSA Finance Center (neither by mail nor via electronic submission).

22. GROSS SHIP WEIGHT

23. SHIPPING POINT

See Block 6

24A. FOR INQUIRIES REGARDING PAYMENT CONTACT:

KC Finance Accounts Payable

24B. TELEPHONE NUMBER

1-800-676-3690

25A. NAME AND TITLE OF OFFEROR/CONTRACTOR

(b) (6), Principal

26A. UNITED STATES OF AMERICA *(NAME OF CONTRACTING/ORDERING OFFICER)*

David J Medina

| (b) (6) | 25C. DATE SIGNED | 26B. SIGNATURE | 26C. DATE SIGNED |
|---|---|---|---|
| | 09/29/2022 | (b) (6) | 09/28/2022 03:55:12 PM EDT |

# Capacity Building Strategic Planning Services and Solutions In Support of the Department of Homeland Security's (DHS) Cybersecurity Infrastructure Security Agency (CISA), Cybersecurity Division (CSD) Capacity Building (CB) Subdivision

**Updated 07.25.2022**

# 1 BACKGROUND

The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure. By connecting stakeholders in industry and government to each other and to resources, analyses, and tools to help them build their own cyber, communications, and physical security and resilience, in turn helping to ensure a secure and resilient infrastructure for the American people. CISA's cybersecurity mission has three primary aspects. First, conduct operations to actively defend cyberspace and help the nation respond to significant incidents. Second, build resilience by addressing systemic risk and helping organizations—particularly those performing National Critical Functions (NCFs)— operate safely and reliably even when being targeted by adversary activity. Lastly, set the conditions that contribute to the vitality and health of the cyber ecosystem. CISA works with its partners to defend against today's threats and collaborates to build more secure and resilient infrastructure for the future. The federal enterprise depends on information technology (IT) systems and computer networks for essential operations. CISA, through its Cyber Security Division (CSD), works with each Federal Civilian Executive Branch (FCEB) agency to promote the adoption of common policies and best practices that are risk-based and able to effectively respond to the pace of ever-changing threats.

CSD leads efforts to protect the federal ".gov" domain of civilian government networks and to collaborate with the private sector - the ".com" domain - to increase the security of critical networks. The CSD mission is to understand evolving threat activity as it affects national critical functions and high value assets, ensuring stakeholder access to essential data on the risk posture of key information systems.

Within CSD, Capacity Building (CB) helps stakeholders better manage cybersecurity risk by defining expectations for stakeholder cybersecurity; leading implementation and enforcement of cybersecurity requirements; managing CISA's cybersecurity services portfolio; and building capacity and enhance collective defense/readiness. CISA provides capacity building, technical assistance, tools, exercises, training programs, and awareness efforts that improve understanding of common risks and possible mitigation strategies for the critical infrastructure community.

## 1.1 CAPACITY BUILDING

Capacity Building serves as CISA's enterprise cybersecurity services management arm for national stakeholders and the lead for federal enterprise cybersecurity governance. CB enables its customers to manage cybersecurity risk by building their capacity to implement effective cybersecurity policies, tools, and procedures. CB executes its mission through four mission lines:

> **Cybersecurity Oversight and Enablement** directs and oversees the implementation of cybersecurity policies and practices and enables customers to take focused, direct actions to meet cybersecurity priorities. It includes work to set Directives, develop guidance and reference architectural products, measure performance and drive accountability with mandates and requirements, and offer targeted engagement and support.

**Cybersecurity Capability Implementation** defines requirements and baselines for a wide range of cybersecurity capabilities and directly implements best-in-class tools for our customers to improve their cyber programs and operations. This work is executed through the Continuous Diagnostics and Mitigation (CDM) Program, which is advancing both core capabilities like Asset Management and more advanced priority capabilities like Endpoint Detection and Response (EDR).

**Cybersecurity Shared Services** identifies, prioritizes, and makes available a robust marketplace of cybersecurity shared service offerings aligned to customer needs and requirements. This includes the work of the Cyber Shared Services Office (formerly the Cyber Quality Service Management Office), the governance model for federal shared services, and will be maturing both the organizational structure and scope of services and customers as it moves forward.

**Cybersecurity Education and Training** addresses today's cyber workforce challenges through innovative education and training opportunities. This includes directly developing and delivering curriculum in priority areas like Incident Response and catalyzing and amplifying training offered through other partners like through the non-traditional training provider grant program.

CB helps stakeholders better manage cybersecurity risk by defining expectations for stakeholder cybersecurity; leading implementation and enforcement of cybersecurity requirements; managing CISA's cybersecurity services portfolio; building capacity; and enhancing collective defense and readiness. Specifically, CB enhances stakeholder cybersecurity readiness, bolsters enterprise capabilities and protections, and increases the community's capacity to adequately manage cyber risk by:

Defining critical requirements needs and performance expectations. Overseeing and guiding the implementation of key cybersecurity initiatives and urgent actions. Managing CISA's cybersecurity services portfolio; evolving shared services, capabilities, and delivery models; and delivering tailored services and assistance based on customer needs.

## 2 PURPOSE

The challenge in today's federal cybersecurity landscape lays in the inconsistencies of programs, service offerings, resources, and standards. As CISA evolves from the nation's risk advisor to working to proactively reduce risk, CB is specifically focused on equipping customers (i.e., building their capacity) to manage cybersecurity risks and increase resilience to everchanging threats. As such, the purpose of this Task Order (TO) is to provide CISA/CSD/CB leadership with the highest quality impactful cybersecurity strategic planning services and solutions.

## 3 SCOPE

The scope of this TO is to provide expert cyber and consulting services that includes, but is not limited to capability-based assessments, organizational structure analysis, legal authorities study and expansion recommendations, service delivery model assessments, strategic roadmap development and functional requirements and standards traceability analysis. The contractor shall

deliver expert Cyber and consulting services as well as those who can advise and assist on critical organizational and technical cyber challenges facing the Federal landscape.

While the preponderance of support will be focused on the Capacity Building mission within CISA, the contractor shall expect to interface with other CSD entities and may be required to directly support CSD leadership with ad hoc projects during this period of performance (PoP). Specifically, the government may experience abrupt shifts in focus driven by Federal Executive leadership. To meet this dynamic need, the contractor shall be capable and prepared to adequately support with requisite technical and IT/Management subject matter expertise and experience.

# 4 TASK AREA REQUIREMENTS AND OBJECTIVES

The below task areas encompass the minimum, yet non-exhaustive, set of objectives for this consulting effort. The objectives are comprised of the various outputs and recommendations and have been mapped to the high-level task areas below. Other objectives, focus areas, and projects may be added throughout the period of performance (PoP) or at the discretion of the government.

## 4.1 TASK 1 –PROJECT MANAGEMENT

The contractor shall provide project management support under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this PWS. The contractor shall identify a Project Manager (PM) by name who shall provide management, direction, administration, quality assurance, and leadership of the execution of this TO.

The contractor shall use industry-best standards and proven methodologies that ensure all TO activities are identified, documented, and tracked so that the TO can continuously be evaluated and monitored for timely and quality service. The contractor shall notify the Contracting Officer (CO) and Contracting Officer's Representative (COR) of any technical, financial, personnel, Organizational Conflict of Interest (OCI), or general managerial problems encountered throughout the life of the TO.

The contractor shall facilitate Government and contractor communications and all activities necessary to ensure the accomplishment of timely and effective support, performed in accordance with the requirements contained in this TO.

### 4.1.1 CONDUCT KICK-OFF AND SCOPING MEETING

The contractor shall schedule and coordinate a Project Kick-off Meeting within two (2) weeks after TO award (TOA) in the National Capital Area (NCR) at a location approved by the Government. The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, and logistic issues; travel authorization; and reporting procedures. At a minimum, the attendees shall include key contractor personnel, TPOC, Functional Leads, key Government representatives, and the Contracting Officer (CO), and COR. The contractor shall provide a Kick-Off Meeting Agenda **(Deliverable 01)** to include, but is not limited to the following:

- Introduction of personnel

- Overview of project tasks
- Overview of organization (complexity)
- Schedule (shows major tasks, milestones, and deliverables; planned and actual start and completion dates for each)
- Communication Plan/lines of communication overview (between both contractor and Government)
- Draft Project Plan
- Travel notification and processes
- Government-furnished information (GFI)
- Security requirements (Building access, badges, etc.)
- Invoice procedures
- Monthly meeting dates
- Reporting Requirements, e.g., Monthly Status Report (MSR), Financial Reporting, etc.
- POCs
- Roles and Responsibilities
- Prioritization of contractor activities
- Any initial deliverables
- Other logistic issues
- Sensitivity and protection of information
- Additional issues of concern (Leave/back-up support).

The contractor shall provide a draft copy of the agenda for review and approval by the COR prior to finalizing. The Government will provide the contractor with the number of participants for the kick-off meeting and the contractor shall provide sufficient copies of the presentation for all present **(Deliverable 02).**

### 4.1.2 PREPARE AND UPDATE PROJECT PLAN

The contractor shall prepare and update the project plan. The Government shall identify emerging projects, objectives, outcomes, artifacts, inputs required, outputs expected (i.e., additional deliverables) which shall be defined and codified in the Project Plan by the contractor. The Initial Draft Project Plan shall be part of the Kickoff presentation. This draft plan will largely identify objectives listed in this contract and any initial assumptions or clarifications. This initial draft plan will also display the notional format for the project's artifact. Post-Kickoff, the contractor shall meet with CB government stakeholders to identify specifications for the various projects. The scoping meetings shall support the first iteration of consulting efforts that shall be codified in the Updated Project Plan (**Deliverable 08**) and provided to the Government NLT 30 calendar days post-award. Project Plan includes scope of consulting efforts being executed. Project Plan includes schedule of milestone, dependencies, and associated project artifacts, outputs, and recommendations. This project plan shall catalog the analyses, projects and studies required by CB stakeholders and sequence them across a schedule within the contract PoP.

### 4.1.3 PREPARE MONTHLY STATUS REPORTS (MSR)

The contractor shall prepare, develop and deliver a MSR **(Deliverable 03)** using Microsoft (MS) Office Suite applications by the tenth ($10^{th}$ ) of each month or the following business day (if the $10^{th}$ falls on a Saturday or Sunday) via electronic mail (email) to the COR**.** The report shall

briefly summarize, by task, the management and technical work conducted during the month. The contractor shall provide at a minimum the following information:

- Activities during reporting period, by task and Subtask to include On-going activities, new activities, activities completed, deliverables submitted for that period; and progress to date on all above-mentioned activities. Start each section with a brief description of the task.
- Problems and corrective actions taken. Also include issues or concerns that may affect project milestones, personnel, and cost resources and proposed resolutions to address them to include risk mitigation plans.
- Personnel gains, losses, and staffing status (upcoming leave, etc.) (LH only).
- Government actions required (deliverables awaiting Government approval, etc.).
- Schedule (from the Project Plan shows major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
- Summary of trips taken, conferences attended, etc.
- Projected cost of each CLIN broken-down by Task and Subtask for the current month for tracking purposes.
- Financial status including (LH only):
    - Chart reflecting funding and burn rate for the month and cumulative
    - Cumulative invoiced costs for each CLIN and Labor Tasks totals to-date.
- A list of current deliverables and milestones generated from the Project Plan identifying deliverable due dates. The list shall identify deliverables and milestones submitted for the period by task as well as provide a projection for the following three (3) months.
- Recommendations for change, modifications, or improvements in task or process.

The contractor shall reconcile the MSR with each monthly invoice.

### 4.1.4 PREPARE TRIP REPORTS

The Government will identify the need for a Trip Report (if required) when a request for travel is submitted. The contractor shall submit Trip Reports five (5) working days after completion of a trip for all long-distance travel **(Deliverable 04).** The contractor shall provide summary of trip in consumable format (i.e., word, excel, ppt. etc.)

The Trip Report will include as a minimum the following information:

- Personnel traveled
- Dates of travel
- Destination(s)
- Purpose of trip
- Cost of the trip
- Approval authority
- Summary of events, action items and deliverables

The contractor shall keep a historical summary of all long-distance travel, to include, at a minimum, the name of the employee, government approval authority, and location of travel, duration of trip, total cost, and purpose.

### 4.1.5 PREPARE MEETING REPORTS

The Government will identify the need for a Meeting Report (if required) when a meeting is scheduled. The contractor shall prepare and submit Meeting Reports to document results of meetings **(Deliverable 05)** one (1) working day following the competition of each meeting. The Meeting Report shall include as a minimum the following information:

- Meeting attendees and their contact information – at minimum identify organizations represented
- Meeting dates
- Meeting location
- Purpose of meeting
- Summary of events, action items and deliverables

The contractor shall ensure their Meeting Reports align with any official meeting minutes if published and submit to the COR accordingly.

### 4.1.6 PREPARE PROBLEM NOTIFICATION REPORTS (PNRs)

The contractor shall prepare and submit a Problem Notification Report (PNR) one day after the problem is identified **(Deliverable 06)** to notify the COR of TO issues such as potential cost/schedule overruns/impacts, assumptions upon which tasks were based that have changed or were incorrect, etc. The PNR shall be prepared in accordance with the sample provided during the kickoff meeting and include a plan detailing the proposed resolution.

### 4.1.7 PROVIDE FINANCIAL REPORTING

The contractor shall provide a Financial Report of cumulative expenditures monthly (**Deliverable 07**) to the COR. The Financial Report shall include as a minimum the following:

- Project monthly expenditures and labor hours by CLIN and TO level starting with the current month through the end of the POP.
- Funded levels by CLIN
- Labor hours incurred to date by CLIN
- Diagram reflecting funding and burn rate by month
- Cumulative invoiced amounts for each CLIN up to the previous month.
- Forecast Estimate to Complete
- Invoice back-up and supporting documentation.

The contractor shall present a Financial Report format at the Project Kick-Off Meeting for Government review. The Government will provide written approval of the proposed format via the COR, and this approved format shall be utilized for the monthly financial reporting requirement. The Government may request updates to the format based on CB requirements.

### 4.1.8 ACCOUTING FOR CONTRACTOR SUPPORT

CB operates and maintains a secure data collection where the contactor shall report ALL contract manpower (including any subcontractor or teaming partners) required for performance of this TO. The contractor shall completely and accurately fill in all the information in the format using the template provided during the kickoff meeting and provide the information to the COR and update throughout the period of performance. All contractor personnel supporting this effort shall be accounted for in the Manpower Database

## 4.2 TASK 2 -SUPPORT STRATEGIC PLANNING EFFORTS AND ORGANIZATIONAL ALIGNMENT

To ensure mission success, CSD and the CB sub-division require comprehensive strategic recommendations for the organizational structure and methods for enterprise performance management. The contractor shall be responsible for conducting the organizational analyses and assessments that will enable CB's rapid maturation. Tasking may include:

- Conduct leadership and staff sessions to align CB on a unified theme, expectations, and outcomes and develop processes to incorporate appropriate perspectives into strategic decisions, mission, and priorities.
- Develop and present for leadership approval a centralized CB operating plan including clear goals, objectives, incentives, and priorities. (**Deliverable 09**) CB Operating Plan objectives and specifications are clearly mapped in the Project Plan. Edits and comments in the project plan shall be incorporated into the Operating Plan.
- Conduct Long Term Planning and future year strategy planning. Planning activities shall include ongoing evaluation via surveys, needs assessments, and interviews of existing services, programs, people, and outcomes.
- Conduct performance management to track how the organization is doing against the annual plan, measuring/reporting success, and identifying opportunities to improve.
- Review, evaluate, distill, and synthesize internal and external data to uncover issues, identify trends and provide insights that drive organizational strategy
- Work with stakeholders across functions and at various levels to assist in solving challenging problems. Support includes developing success metrics, measuring results, and integrating new methodologies into existing systems.
- Identify organizational investments in people, technology, and capital connected to higher division strategies.
- Advise, assist, and support on external engagements.

## 4.3 TASK 3 -PROVIDE STRATEGIC INITIATIVES CONSULTING SUPPORT

Recent cyber-attack campaigns have underscored the critical need to assist agencies in identifying the most significant cybersecurity risks and driving timely remediation of security weaknesses and overall improvement in cyber risk capabilities and posture across the federal enterprise. Remediation efforts on the heels these incidents have also highlighted gaps in the way that CSD and CB assists agencies, with a need to better bridge operational and programmatic support activities executed by each of the Divisions/Subdivisions within the organization to achieve continuity and build upon progress. The government requires vision and planning support to strategic initiatives and work groups associated with delivering capability to

the federal enterprise. The contractor shall assist with developing and designing strategic plans in accordance with changes in the operating landscape, priorities, and initiatives of the organization. Responsibilities and objectives include but are not limited to the following:

- Drive/support key leadership initiatives either at agency, cross agency, or external partner level. Support may include important ad-hoc critical initiatives or projects identified by leadership priorities (e.g., Ransomware, Identity Management, etc.).
- Targeted ad-hoc requests and/or static reporting focused on distilling information into insights to support leadership decisions and growth (e.g., new legislation, Executive Orders (Eos), agency plans, research, external trends, etc.)
- Support external strategy work (e.g., CSD Front Office, CISA Strategy, Policy and Plans, Office of National Cyber Director, Office of Management and Budget) by helping coordinate necessary requests, and ensuring any requirements or deliverables associated with the task are completed.

The contractor shall be capable of deploying flexible team(s) to coordinate, introduce, participate, or plan organizational initiatives, task forces or working groups.

### 4.4 TASK 4 -PERFORM STRATEGIC, TACTICAL AND OPERATIONAL PLANNING SUPPORT

Synergy and program integration are vital to the efficacy of large organizational units, the contractor shall provide the subject matter expertise needed to assist CB in evaluating and/or implementing action plans, which ensure integration of their multiple operational programs. Support includes growth initiatives, continuous process improvement and establishing processes and best practices. The contractor shall provide support including the following, and additions as mutually agreed upon. Plan, manage, and develop recommendations from concept to launch to meet key milestones and mission needs for government approval.

- Execute research that helps programs better understand organizational needs to inform improvements to products, services, policies, and processes.
- Provide cross cutting support to ongoing CSD and CB standards and metrics development efforts
- Develop template roadmaps and integration plans for current CISA cybersecurity services, to include, where applicable, standards and requirements identification and baselining by the CISA Standards Area Lead
- Evaluate, coordinate, research, analyze, and develop action plans in support of the execution of current or prospective programs and/or execution of project implementation.
- Conduct assessments and studies of potential initiatives and well as hands on implementation
- Perform problem solving, development of correction and/or enhancement plans, and implementation of those plans on an as needed basis
- Assist in achieving internal and external consensus.
- Support the development and management of organizational strategic guidance documents, to include Goals, Objectives, and Key Milestones (e.g., Annual Operating Plan).

## 4.5 TASK 5 - CSSO STRATEGIC GROWTH SUPPORT

The CSSO requires strategy and strategic governance support on existing and new initiatives to ensure enterprise-wide alignment for the FCEB, as well as potential inclusion of SLTTs. The contractor shall support the following taskings to include, but is not limited to the following:

- Engage with CISA leadership, stakeholders, and customers to identify and prioritize CSSO initiatives and governance backlog requiring support (**Deliverable 11**) CSSO Backlog objectives, schedule and specifications shall be clearly mapped in the Project Plan. Edits and Comments in the Project Plan shall be incorporated into the Operating Plan
- Develop CSSO strategy and strategic governance concepts to support organizational growth and maturity
- Produce written and graphics-based deliverables (e.g., roadmaps, strategic plans, playbooks, concepts of operations) to define, memorialize, and mature CSSO operations
- Spearhead development of the CSSO strategic governance backlog.
- Provide expertise and analysis around stakeholder feedback to uncover opportunities to stimulate growth of the CSSO.
- Provide strategy mapping expertise to ensure all CSSO strategy, governance, and program management efforts are in alignment with CB, CSD, and CISA strategies.
- Build partnerships across CSD to identify impact, dependencies, and/or risks to the CSSO Program Roadmap.
- Support executive leadership briefings and provide insights on impact to CSSO mission.
- Assist and support with the development of a Value Stream
- Inform the CSSO Enterprise Architecture including the development of value streams and/or proposition statements.
- Identify and catalog upstream and downstream dependencies.

## 4.6 TASK 6 - CYBER THREAT INTELLIGENCE AS A SERVICE (CTIaaS) (OPTIONAL)

The Cyber Shared Services Office (CSSO) requires strategic planning support to assist in the development of the Cyber Threat Intelligence as a Service (CTIaaS) initiative. The contractor shall support the following taskings to include, but is not limited to the following:

- Develop CTIaaS technical strategy and roadmap in alignment with applicable CSSO, CB, and CSD strategies and roadmaps and in coordination and collaboration with CSD operational teams and CISA's external partners and stakeholders. (Deliverable 10) The CTIaaS strategy and roadmap objectives, schedule and specifications shall be clearly mapped in the Project Plan. Edits and comments from the project plan shall be incorporated into the Operating Plan.
- Develop short- and long-term strategic approach, execution and communication plans for existing cyber threat intelligence capabilities and services in alignment with other higher-level technical strategies and roadmaps.
- Produce written and graphics-based deliverables (e.g., roadmaps, technical strategy, implementation plans, communication plans, service delivery models, service architecture and design).

- Build partnerships across CSD to identify impact, dependencies, and/or risks to the CTI technical roadmap.
- Support executive leadership briefings and provide insights on impact to CTI mission.

### 4.7 TASK 7 - CDM STRATEGIC PLANNING SUPPORT (OPTIONAL)

The contractor shall provide the strategic planning support. OMB has directed the CDM Program Office to perform a program review of CDM and incorporate lessons learned into a strategy to continue improving the program. This strategy will articulate challenges and opportunities for improving delivery, data quality, and support for automation.

CDM requires support in defining a high-level program review covering the next five years. The strategic planning support shall include, but not be limited to the following:

As a ten-year old cyber program, how can it evolve to offer flexibility for ever changing cyber requirements?

- What organizational structure would set it up for success?
- Given the strong role CISA plays on the federal cyber landscape, how should CDM meet both internal and external stakeholder needs?
- Given other CISA cyber programs, how would CDM best integrate without overlapping?
- What other funding options for cyber capabilities/tools might be more effective than the traditional base plus one year [with exception of CDM Shared Services for non-CFO Act agencies):
- Given the emerging role of endpoint visibility for both agencies and CISA how can CDM evolve to ensure CDM data is leveraged, available and useful?

Deliverables would include the proposed approach, master schedule and up to five, or more reports covering agreed upon topics including and additions as mutually agreed upon. to the above focus areas. The contractor shall assist the Government in developing and defining the program review focusing on near-term (one year), -term mid (three years) and long term (five years and beyond) strategy.

### 4.8 TASK 8 -PROVIDE SURGE SUPPORT (OPTIONAL)

The contractor shall provide surge support. This task supports emerging projects that fall within the above task areas. As the cybersecurity environment is dynamic, complex, and continuously evolving the Government anticipates the need to surge throughout the PoP to efficiently meet evolving program and mission changes and challenges. Projects and support will be identified in a new work project plan, approved by the Government and COR and executed through the Surge CLIN.

## 5 DELIVERABLE AND OBJECTIVE MAPPING

| # | Deliverable | Date Due/Frequency | Task Reference or Description |
|---|---|---|---|
| 1 | Contract Kickoff Agenda | 5 Days After Award | Task 1; Provide kickoff agenda topics in PowerPoint slide form |

| | | | |
|---|---|---|---|
| 2 | Kick-off Presentation | NLT 15 after Award; 2 days prior to kickoff presentation | Task 1; Develop and deliver Contract Kick-off Slide deck. Provide as a read-ahead 2 days prior to presentation |
| 3 | Monthly Status Report | Every 10th day of the month post-award | Task 1; Develop monthly status report in accordance with description in Task 1 as well as any other pertinent information identified by the government at time of award |
| 4 | Trip Report | 5 days after trip | Task 1; Provide summary of trip in consumable format (i.e., word, excel, ppt. etc.) |
| 5 | Meeting Reports | 1 day after meeting | Task 1; meeting report minutes and summary in consumable format |
| 6 | Problem Notification Report | Within 1 day of identifying issue and/or problem | Task 1; word document summarizing issue to include government actions required (if applicable) |
| 7 | Financial Report | Submitted monthly along with every invoice | Developed in accordance with Task 1 |
| 8 | Project Plan | Initial Project Plan provided 30 days after contract award<br>Updates to project plan will occur as new activities or projects are identified by the government | Task 1; Developed in word. Government shall identify projects aligned to Task areas to include objectives, outcomes, artifacts, inputs required, outputs expected (i.e., additional deliverables). This project plan will include schedule and dependencies. |
| 9 | CB Operating Plan | Draft 180 days post award<br>Final 270 days post award | Task 2 |
| 10 | CTIaaS Technical Strategy and Roadmap | 180 days upon execution of optional CLIN | Task 6 |
| 11 | CSSO Initiatives and Governance Priority Backlog | 180 days post award | Task 5 |

## 6 PERFORMANCE PERIOD

Base period will be 12 months with four (4) twelve-month option periods and the possibility to a 6-month extension IAW with FAR 52 217-8. The base period will include a minimum set of project deliverables and objectives. Award terms for option periods will be contingent upon 1) how successful the contractor is in delivering the base year projects and objectives and 2) CSD and CB portfolio needs. Option period terms will delineate a new set of work plans and projects as required.

There is no minimum guaranteed level of compensation or support beyond the base period. The government may add projects and ad hoc support at any time. 90 days prior to the end of the Base Period the government will notify the contractor of their intent to award the option period, to include new or extended objectives for specified projects and/or additional support.

## 7 PLACE OF PERFORMANCE

The primary place(s) of performance at Task Order Award (TOA) is at contractor's facility due to the current circumstances of the national pandemic.

During the PoP of the TO and as the workplace circumstances evolve the contractor shall perform the TO requirements on-site at the government's facility located in Ballston, VA and off-site at the contractor facility. An on-site support schedule may be identified post-award. It is preferred that the contractor's facility be within the Washington DC metro area/NCR and near the Government's location in Arlington, VA (Ballston area). The contractor shall be required to routinely travel to the to the Government's location in Arlington, VA (Ballston area). The contractor's facility shall include conference and meeting room space and support routine Government meetings and events.

## 8 OTHER DIRECT COSTS (ODCs)

ODCs will be reimbursed at cost.

## 9 TRAVEL

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

a. FTR - prescribed by the GSA, for travel in the contiguous U.S.
b. DSSR (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" - prescribed by the Department of State, for travel in areas not covered in the FTR.

Before undertaking travel to any Government site or any other site in performance of this TO, the contractor shall have this travel and coordinated with the CISA Functional Lead and approved by the COR. Notification shall include, at a minimum, the number of persons in the party, traveler name, destination, duration of stay, purpose, and estimated cost. Prior to any long-distance travel, the contractor shall prepare a TAR for Government review and approval. Government will provide a sample during the kickoff meeting. Long distance travel will be reimbursed for cost of travel comparable with the FTR and DSSR.

Requests for travel approval shall:

a. Be prepared in a legible manner.
b. Include a tracking ID number
c. Include a description of the travel proposed including a statement as to purpose
d. Be summarized by traveler.
e. Identify the TO number.
f. Identify the CLIN associated with the travel.
g. Be submitted in advance of the travel with sufficient time to permit review and approval.

The contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Travel shall be scheduled during normal duty hours whenever possible.

## 10 ROLES AND RESPONSIBILITIES

Identification of all government personnel, including their specific roles and responsibilities:

**Contracting Officer**

GSA FAS R8 Contracting Officer

*Responsibility for contracting activities rests solely with the Government Contracting Officer. No conversation, recommendations, or direction, whether given directly by, or implied by Government personnel, that will affect the scope, schedule, or price of the program covered by this solicitation or any resulting contract, shall be acted upon by the Contractor unless specifically approved by the Government Contracting Officer. In the absence of the assigned CO, any GSA Region 8 CO may fill in and has full authority to act on this task order.*

**Contracting Specialist**

GSA FAS R8 Contracting Specialist

*As a member of the contract administration team, the contract specialist will be responsible for working in concert with the Contracting Officer while performing post award administrative functions and certain assigned pre-award functions.*

**Contracting Officer's Representative (COR)**

CISA Contracting Officer's Representative (COR)

*CONTRACTING OFFICER'S REPRESENTATIVE (DEC 1991)*

*(a) Definition. "Contracting officer's representative" means an individual designated in accordance with subsection 201.602-2 of the Defense Federal Acquisition Regulation Supplement and authorized in writing by the contracting officer to perform specific technical or administrative functions.*

*(b) If the Contracting Officer designates a contracting officer's representative (COR), the Contractor will receive a copy of the written designation. It will specify the extent of the COR's authority to act on behalf of the contracting officer. The COR is not authorized to make any commitments or changes that will affect price, quality, quantity, delivery, or any other term or condition of the contract.*

## 11 GOVERNMENT-FURNISHED EQUIPMENT (GFE) AND GOVERNMENT FURNISHED INFORMATION (GFE/GFI)

The Government will provide the contractor with DHS LAN-A accounts. The contractor will not be required to receive DHS laptops or other equipment.

The Government will provide all necessary information, data, and documents to the Contractor for work required under this contract. The Contractor shall use Government furnished information, data, and documents only for the performance of work under this contract and shall be responsible for returning all Government furnished information, data, and documents to the Government at the end of the performance period. The Contractor shall not release Government furnished information, data, and documents to outside parties without the prior written consent of the Contracting Officer.

The contractor shall protect all GFI (e.g., Government data) by treating the information as Sensitive But Unclassified (SBU). SBU information and data shall only be disclosed to

authorized personnel as described in the TO herein. The contractor shall keep the information confidential and use appropriate safeguards to maintain its security in accordance with minimum Federal standards.

When no longer required, this information and data shall be returned to Government control, destroyed, or held until otherwise directed by the GSA CO. The contractor shall destroy unneeded items by burning, shredding, or any other method that precludes the reconstruction of the material.

If work under this TO requires that the contractor's personnel have access to Privacy Information, contractor personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code, section 552a and applicable Agency rules and regulations.

## 12 CONFIDENTIALITY OF DATA

The contractor is required to comply with FAR 9.505-4(b), A contractor that gains access to proprietary information of other companies in performing advisory and assistance services for the Government must agree with the other companies to protect their information from unauthorized use or disclosure for as long as it remains proprietary and refrain from using the information for any purpose other than that for which it was furnished. The contracting officer shall obtain copies of these agreements and ensure that they are properly executed. Duplication or disclosure of the data and other information to which the contractor develops or will have access to as a result of this TO is prohibited. It is understood that throughout performance of this TO, the contractor will have access to confidential data, which either is the sole property of the DHS or is the sole property of other than the contracting parties. The contractor and its subcontractor(s) (if any) agree to maintain the confidentiality of all data to which access may be gained throughout task order performance, whether title thereto vests in DHS or otherwise. The contractor and his subcontractor(s) (if any) agree to not disclose said data, any interpretations and/or translations thereof, or data derivative there from, to unauthorized parties in contravention of these provisions, without the prior written approval of the CO and the party in which title thereto is wholly vested. Subcontractors are subject to the same stipulations and may be held responsible for any violations of confidentiality.

## 13 ORGANIZATIONAL CONFLICT OF INTEREST (OCI)

a. If a contractor has performed, is currently performing work, or anticipates performing work that creates or represents an actual or potential OCI, the contractor shall immediately disclose this actual or potential OCI to the CO in accordance with FAR Subpart 9.5. The nature of the OCI may involve the prime contractor, subcontractors of any tier, or teaming partners.

b. The contractor is required to complete and sign an OCI Statement. The contractor must represent either that (1) It is not aware of any facts which create any actual or potential OCI relating to the award of this contract, or (2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential OCI and has included a mitigation plan in accordance with paragraph (c) below.

c. If the contractor with an actual or potential OCI believes the conflict can be avoided, neutralized, or mitigated, the contractor shall submit a mitigation plan to the Government for review.

d. In addition to the mitigation plan, the CO may require further information from the contractor. The CO will use all information submitted by the contractor, and any other relevant information known to GSA, to determine whether an award to the contractor may take place, and whether the mitigation plan adequately avoids, neutralizes, or mitigates the OCI.

e. If any such conflict of interest is found to exist, the CO may determine that the conflict cannot be avoided, neutralized, mitigated, or otherwise resolved to the satisfaction of the Government, and the contractor may be found ineligible for award. Alternatively, the CO may determine that it is otherwise in the best interest of the U.S. to contract with the contractor and include the appropriate provisions to avoid, neutralize, mitigate, or waive such conflict in the contract awarded.

f. This effort will involve providing technical and programmatic assistance and advice, potentially resulting in of the development contract documentation (Statements of Work (SOWs) and other acquisition documents), and access to proprietary and/or sensitive Government and contractor information. The contractor shall be precluded from bidding on any future requirements for which it supported the preparation development of any acquisition documentation. The contractor shall comply with the requirements under FAR Subpart 9.5 Organizational and Teaming/Consultant Conflicts during performance under this Task Order.

## 14 KEY PERSONNEL

The following are the minimum personnel who shall be designated as "Key." The Government does not intend to dictate the composition of the ideal team to perform this TO. The Government will evaluate up to three additional Key Personnel as proposed by the contractor.

The key personnel for this TO shall be:

a) Program Manager (PM). The contractor shall identify a PM to serve as the Government's main POC and to provide overall leadership and guidance for all contractor personnel assigned to the TO. The PM shall ultimately be responsible for the quality and efficiency of the TO. The PM shall have organizational authority to execute the requirements of the TO. The PM shall assign tasking to contractor personnel, supervise ongoing technical efforts, and manage overall TO performance to ensure the optimal use of assigned resources and subcontractors. This Key Person shall have the ultimate authority to commit the contractor's organization and make decisions for the contractor's organization in response to Government issues, concerns, or problems. The PM shall be readily available to respond to Government questions, concerns, and comments, as well as be proactive in alerting the Government to potential contractual and programmatic issues.

The PM shall possess all required qualifications (below) at time of proposal submission:

a. At least five years of experience managing and supervising staff and leading multi-disciplinary teams on performance-based projects similar to the TO scope.
b. At least 10 years of Experience in completing, leading, or directing the work of others on projects similar to the size, scope, and complexity of the work and environment described above.
c. Managerial experience providing technical advice, organizing, planning, directing, and

managing staff to ensure goals and objectives are achieved.

d. Experience with risk management, issue resolution, problem solving, and customer service.
e. Current Project Management Institute (PMI) Project Management Professional, Program Management Professional certification, or MBA.

# 15 SECURITY REQUIREMENTS

## 15.1 GENERAL

The Government requires all information pertaining to this TO be stored and protected in accordance with Government policy regarding SBU information. Therefore, no information shall be stored or transmitted outside the U.S. The information associated with this TO is critical infrastructure information as defined by 1016(e) of the U.S. Patriot Act of 2001 (42 U.S.C. 5195c(e)).

DHS security requirements are also applicable to this TO. In some instances, the contractor shall have to follow specific Agency security requirements that will be provided post-award as GFI.

## 15.2 FACILITY CLEARANCE LEVEL (FCL)

At the time of proposal submittal, the contractor shall have a contractor facility with an approved facility clearance at the Top Secret (TS) level. Although the TO utilizes information at the SBU level, the FCL will allow for greater classification levels as directed by the Government.

An FCL is an administrative determination that, from a national security standpoint, a facility is eligible for access to classified information at the Confidential, Secret, or TS level. The FCL includes the execution of a DoD Security Agreement (DD Form 441 and DD Form 441-1) and Certificate Pertaining to Foreign Interests (Standard Form (SF) 328). Under the terms of an FCL agreement, the Government agrees to issue the FCL and inform the contractor as to the security classification of information to which the contractor will have access. The contractor, in turn, agrees to abide by the security requirements set forth in the National Industrial Security Program Operating Manual (NISPOM).

In general, all necessary FCLs shall be at the expense of the contractor.

## 15.3 ACCESS TO AND PROTECTION OF CLASSIFIED INFORMATION

The contractor shall ensure these instructions are expressly incorporated into any and all subcontracts or subordinate agreements issued in support of this contract.

Performance on this contract requires the contractor to gain access to classified National Security Information (includes documents and material), which mandates protection in accordance with Executive Order 13526 National Security Information (NSI), as amended, as well as any supplemental directives.

The contractor shall abide by the requirements set forth in the DD Form 254, Contract Security Classification Specification **(Attachment X);** the National Industrial Security Program Operating Manual (NISPOM), as well as any relevant Intelligence Community Directives (ICDs)

for protection of classified and/or compartmented information at its cleared facility, if applicable, or as further directed by the Special Security Officer (SSO)/Office of Selective Acquisition Security Manager (OSASM). If the contractor is required to have access to classified information at any DHS or other government facility, it shall abide by the security requirements set forth by the Cognizant Security Authority (CSA) for that facility.

## 15.4 PERSONNEL SECURITY CLEARANCES

At time of award (TOA), only the contractor's PM and DPM contractor personnel shall possess a TS-SCI security clearance. The Government will dictate the need for any additional security clearance requirements when applicable.

At a minimum all contractor staff are required to have DHS Suitability.

In general, all necessary employee security clearances shall be at the expense of the contractor. The contractor shall comply with all security requirements.

## 16 EMPLOYMENT ELIGIBILITY

The contractor will ensure that each employee working on this contract has a Social Security Card issued and approved by the Social Security Administration. The contractor will be responsible to the Government for acts and omissions of its own employees and for any sub-contractor(s) and their employees.

Subject to existing law, regulations and/ or other provisions of this contract, illegal or undocumented aliens will not be employed by the contractor, or with this contract. The contractor will ensure that this provision is expressly incorporated into any and all subcontracts or subordinate agreements issued in support of this contract.

## 17 CONTINUED ELIGIBILITY

DHS reserves the right and prerogative to deny and/ or restrict the facility and information access of any Contractor employee whom DHS determines to present a risk of compromising sensitive Government information to which he or she would have access under this contract.

The Contractor will report to the DHS Security Office any adverse information coming to its attention concerning employees working under this contract. Reports based on rumor or innuendo will not be made. The subsequent termination of an employee does not obviate the requirement of the Contractor to submit this report.

The report will include employee's name, social security number, along with the adverse information being reported.

The Security Office may require drug screening for probable cause at any time and/or when the Contractor independently identifies, circumstances where probable cause exists.

The Security Office must be notified of all terminations/ resignations within 5 days of occurrence. The Contractor will return to the COR any expired DHS-issued identification cards and building passes, or those of terminated employees. If an identification card or building pass is not available to be returned, a report must be submitted to the COR, referencing the pass or

card number, name of individual to whom issued, the last known location and disposition of the pass or card.

## 18 SUITABILITY DETERMINATION

DHS will have and exercise full control over granting; denying, withholding, or terminating unescorted government facility and/or sensitive Government information access for Contractor employees, based upon the results of a background investigation. DHS may, as it deems appropriate, authorize, and make a favorable entry on duty (EOD) decision based on preliminary security checks. The favorable EOD decision is required before employees requiring access to sensitive information will be allowed to commence work prior to the completion of the full investigation. The granting of a favorable EOD decision will not be considered as assurance that a full employment suitability authorization will follow. The granting of a favorable EOD decision or a full employment suitability determination will in no way prevent, preclude, or bar DHS from the withdrawing or terminating access to facilities or information at any time during the term of the contract. No employee of the Contractor will be allowed unescorted access to a Government facility without a favorable EOD decision or suitability determination by the Security Office.

Contractor employees' not needing access to sensitive DHS information, or recurring access to DHS' facilities, will not be subject to security suitability screening.

Contractor employees awaiting an EOD decision may begin work on the contract provided they do not access sensitive Government information. Limited access to Government buildings is allowable prior to the EOD decision if a cleared Government employee escorts the Contractor. This limited access is to allow Contractors to attend briefings, meetings and begin work.

## 19 INFORMATION TECHNOLOGY SECURITY CLEARANCE

When sensitive government information is processed on Department telecommunications and automated information systems, the Contractor agrees to provide for the administrative control of sensitive data being processed and to adhere to the procedures governing such data as outlined in *DHS IT Security Program Publication DHS MD 4300.Pub.* Contractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractors who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

## 20 SECURITY PROCESS

The procedures outlined below shall be followed for the DHS Security Office to process background investigations and suitability determinations, as required, in a timely and efficient manner.

Carefully read the security clauses in the contract. Compliance with the security clauses in the contract is not optional.

Contract employees (to include applicants, temporaries, part-time and replacement employees) under the contract, requiring access to sensitive information, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through the DHS Office of Security/PSD. Prospective Contractor employees shall submit the following completed forms to the DHS Office of Security/PSD Office. The Standard Form (SF) 85P will be completed electronically, through the Office of Personnel Management's e-QIP SYSTEM. The completed forms must be given to the DHS Office of Security no less than thirty (20) days before the start date of the contract or thirty (10) days prior to entry on duty of any employees, whether a replacement, addition, subcontractor employee, or vendor:

a. Standard Form 85P, "Questionnaire for Public Trust Positions"
b. FD Form 258, "Fingerprint Card" (2 copies)
c. DHS Form 11000-6 "Conditional Access to Sensitive but Unclassified Information Non-Disclosure Agreement"
d. DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"

Only complete packages will be accepted by the DHS Security Office. Specific instructions on submission of packages will be provided upon award of the contract.

DHS may, as it deems appropriate, authorize, and grant a favorable entry on duty (EOD) decision based on preliminary suitability checks. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow. A favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar DHS from withdrawing or terminating access to government facilities or information, at any time during the term of the contract. No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable EOD decision or suitability determination by the DHS Office of Security/PSD.

The DHS Security Office shall be notified of all terminations/resignations within five (5) days of occurrence. The Contractor shall return to the Contracting Officer's Representative (COR) all DHS issued identification cards and building passes that have either expired or have been collected from terminated employees. If an identification card and/or building pass is not available to be returned, a report shall be submitted to the COR, referencing the building pass and/or identification card number, name of individual to who it was issued and the last known location and disposition of the building pass and/or identification card.

Failure to follow these instructions may delay the completion of suitability determinations and background checks. Note that any delays in this process that are not caused by the government do not relieve a contractor from performing under the terms of the contract.

Your POC at the Security Office is:

Office of Security/PSD Customer Service Support Washington DC 20528
Telephone: (202) 447-5010

## 21 ADVERTISING, PUBLICIZING AWARDS AND NEWS RELEASES

Under no circumstances shall the contractor, or anyone acting on behalf of the contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any publicity/ news release or commercial advertising without first obtaining explicit written consent to do so from the COR and Contracting Officer.

This restriction does not apply to marketing materials developed for presentation to potential government customers of this contract vehicle.

The contractor agrees not to refer to awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

The contractor shall not make any press/news releases pertaining to this procurement without prior Government approval and only in coordination with the GSA CO and DHS COR.

## 22 NON-PERSONAL SERVICES

The Government and the contractor understand and agree that the services delivered by the contractor to the Government are non-personal services. The parties also recognize and agree that no employer-employee or master-servant relationship exists or will exist between the Government and the contractor. The contractor and the contractor's employees are not employees of the Federal Government and are not eligible for entitlement and benefits given federal employees.

Contractor personnel under this task order shall not (i) be placed in a position where there is an appearance that they are employed by a Federal Officer, or are under the supervision, direction, or evaluation of a Federal Officer, or (ii) be placed in a position of command, supervision, administration, or control over Government personnel.

## 23 CONTRACTOR PERSONNEL

The contractor shall ensure that its staff and subcontractors maintain any generally required professional certifications, accreditations, and proficiency relative to their areas of expertise. The contractor shall retain documentation of such records. The Government will not pay expenses to meet this requirement.

### 23.1 IDENTIFICATION OF CONTRACTOR PERSONNEL

The contractor shall ensure that its employees will identify themselves as employees of their respective company while working on CISA/GSA contracts. For example, contractor personnel shall introduce themselves in person, voicemail, email, and sign attendance logs as employees of their respective companies, and not as CISA employees. The contractor shall ensure that their personnel use the following format signature on all official e-mails generated by CISA computers:

Name
Position or Professional Title Company Name
Supporting the CISA/IP/SOPD/Office of DHS Phone
Other contact information as desired.

## 24 PRINTING RESTRICTIONS

All printing funded by this task order must be done in conformance with Joint Committee on Printing regulations as prescribed in Title 44, United States Code, and Section 308 of Public Law 101-163, and all applicable Government Printing Office and Department of Homeland Security regulations.

## 25 EMPLOYEE IDENTIFICATION

Contractor employees visiting Government facilities shall wear an identification badge that, at a minimum, displays the contractor's name, the employee's photo, name, clearance-level and badge expiration date. Visiting contractor employees shall comply with all Government escort rules and requirements. All contractor employees shall identify themselves as contractors when their status is not readily apparent and display all identification and visitor badges in plain view above the waist at all times.

Government issued identification badge. All contractor employees shall identify themselves as contractors when their status is not readily apparent (in meetings, when answering Government telephones, in e-mail messages, etc.) and display the Government issued badge in plain view above the waist at all times.

## 26 EMPLOYEE CONDUCT

Contractor's employees shall comply with all applicable Government regulations, policies, and procedures (e.g., fire, safety, sanitation, environmental protection, security, "off limits" areas) when visiting or working at government facilities. The contractor shall ensure contractor employees present a professional appearance at all times and that their conduct shall not reflect discredit on the United States or the Department of Homeland Security. The contractor shall ensure its employees understand and abide by Department of Homeland Security established rules, regulations and policies concerning safety and security.

## 26.1 REMOVING EMPLOYEES FOR MISCONDUCT OR SECURITY REASONS

The Government may, at its sole discretion (via the Contracting Officer), direct the contractor to remove any contractor employee from DHS facilities for misconduct or security reasons. Removal does not relieve the contractor of the responsibility to continue providing the services required under this task order. The Contracting Officer will provide the contractor with a written explanation to support any request to remove an employee.

## 27 CONTRACTOR PERSONNEL

## 27.1 NOTIONAL STAFFING REFERENCE

The price proposal template represents notional level of effort, based on historical and forecasted contract support that may be needed for this TO. The contractor shall utilize the price proposal attachment as a reference but shall propose a labor mix or level of effort in support of their solution to meeting the TO requirements that may or may not be in accordance with the attachment.

## 27.2 QUALIFIED PERSONNEL

The contractor shall provide qualified personnel to perform all requirements specified in this PWS.

## 27.3 CONTINUITY OF SUPPORT

The contractor shall ensure that the contractually required level of support for this requirement is maintained at all times. The contractor shall ensure that all contract support personnel are present for all hours of the workday. If for any reason the contractor staffing levels are not maintained due to vacation, leave, appointments, etc., and replacement personnel will not be provided, the Contractor shall provide email notification to the CO, CS, and the COR at least one week prior to employee absence. Otherwise, the contractor shall provide a fully qualified replacement.

## 28 4300A SENSITIVE SYSTEMS

References:

- DHS Management Directive 140-01, "*Information Technology Security Program*
- DHS National Security Systems Policy Directive 4300A, Version 13.1, July 25, 2017
- DHS National Security Systems Policy Directive 4300B, Version 10.1, November 21, 2018' for NSS Collateral (Unclass, Secret or Top-Secret Collateral).
- 'DHS Sensitive Compartmented Information (SCI) Systems 4300C Instruction Manual, Version 2.1, March 24, 2017' for TS SCI/C-LAN.